نظرية الحلقات

المحاضرة الرابعة

العام الدراسي 2024-2025

Prof. DR. Muna Abbas Ahmed

Quotient ring حلقة القسمة

Def. Let R be a ring and Let I be an ideal of R Then R/I is an abelian group where: $R/I = \{r+I / r \in R\}$

Define $\oplus$ and $\odot$ on R/I as following:
شرط التالي .

$$\left.\begin{aligned}(r_1+I)\oplus(r_2+I) &= (r_1+r_2+I)\\(r_1+I)\odot(r_2+I) &= (r_1 r_2+I)\end{aligned}\right\} \forall r_1, r_2 \in R$$

* القسمة لا تصح الا اذا كانت الزمرة الجزئية ابدالية .
* يقبل الرفع الايمن = الايسر الا اذا كانت I مثالية

R/I قسمة , $R \backslash I$ ماعدا

Then $(R/I, \oplus, \odot)$ is a ring whic is called Quotient ring

Prove or disprove :- $\frac{R}{I}$ is always finite $\forall$ an ideal I of ring R. ✗

EX. $R = \mathbb{Z} \oplus \mathbb{Z}$, $I = \mathbb{Z}$, $\frac{R}{I} = \frac{\mathbb{Z}\oplus\mathbb{Z}}{\mathbb{Z}} = \mathbb{Z}$

But $\mathbb{Z}$ is infinte

R finit $\longrightarrow R/I$ finit

س/ هل أن صفات الحلقة R تنتقل الى الحلقة R/I

ج/ ليس بالضرورة (ليس دائماً) والملاحظة الآتية تبين انتقال قسم من هذه الصفات.

Remark :- Let R a ring and let I be an ideal of Then.

① if R is comm. ring Then So is R/I . تبع العملية الثانية

② if R has an identity element 1 Then So is R/I

③ ~~has~~ if R has no Zero diver element may not R/I.

$\boxed{\text{Proof 1}}$

Let $a+I, b+I \in R/I$ we must show That:

$(a+I)(b+I) = (b+I)(a+I)$

$ab+I$ by def of $\odot$ $= (b+I)(a+I)$

$a, b \in R$, and R comm.

$\therefore ab+I = ba+I \Rightarrow (b+I)(a+I)$

$\boxed{\text{Proof 2}}$

We have 1 is The id. of R

claim That $1+I$ identity of R/I So Let $a+I \in R/I$

We must Prove That:

$(1+I)(a+I) = (a+I)(1+I) = (a+I)$

$1\cdot a+I \qquad 1\cdot a+I = a\cdot 1+I = a+I$ by def $\odot$

$\therefore R$ is comm. with any element of R

$\therefore a\cdot 1+I$ by def $\odot$ $\Rightarrow (a+I)(1+I) \qquad a\cdot 1+I = a+I$

③ Prove or dis Prove:-

if R is I.D then R/I is also . X

since: Let $R = Z$, $I = 4Z$

$$R/I = \frac{Z}{4Z} = \{n+4Z \mid n \in Z\}$$

$$= \{0+4Z, \mp 1+4Z, \mp 2+4Z - - -\}$$

$$= \{0+4Z, \mp 1+4Z, \mp 2+4Z, \mp 3+4Z\}$$

$$= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$ has Zero diver

$$R/I = \frac{Z}{4Z} \simeq \underline{\underline{Z_4}}$$

Z_4 not I.D since has Zero diver element
but Z is I.D

In genarl $\frac{Z}{PZ} \simeq Z_P$ is I.D

$\frac{Z}{2Z} \simeq 2Z$, Z is I.D & $\frac{Z}{2Z}$ is I.D

$P = \{Z_2, Z_3, Z_5, Z_7, Z_{11}, Z_{13} - - -\}$

55

EX. Consider The ring of integer number Z, and The ideal nZ of Z, The Quotient ring.

$$\frac{Z}{nZ} = \{r + nZ \mid r \in Z\}$$

$\boxed{\text{if } n = 2}$ So, we have

$$\frac{Z}{2Z} = \{r + 2Z / r \in Z\}$$

$$= \{0 + 2Z, \mp 1 + 2Z, \cdots\}$$

$0 + 2Z = \{0, \mp 2, \mp 4, \mp 6, \mp 8, \ldots\}$

$2 + 2Z = \{2, 4, 0, -2, -4, \ldots\}$

$3 + 2Z =$

$4 + 2Z =$

$5 + 2Z =$

$$= \{0 + 2Z, 1 + 2Z\} = \{\bar{0}, \bar{1}\} = Z_2$$

$$\therefore \frac{Z}{2Z} \simeq Z_2$$

$\boxed{\text{if } n = 3}$ $\frac{Z}{3Z} = \{n + 3Z / n \in Z\}$

$$= \{0 + 3Z, \mp 1 + 3Z, \ldots\}$$

$0 + 3Z = \{0, \mp 3, \mp 6, \mp 4 \ldots\}$

$1 + 3Z =$

$2 + 3Z =$

$3 + 3Z =$

$$\boxed{\therefore \frac{Z}{3Z} \simeq Z_3}$$

$$\frac{Z}{3Z} = \{0 + 3Z, 1 + 3Z, 2 + 3Z\} = \{\bar{0}, \bar{1}, \bar{2}\} = Z_3$$

- أخذنا سابقاً التشاكل (تعريف) سنعرف في أفرسنا التشاكل سيمى (التشاكل الطبيعي).

$\pi : G \to \frac{G}{H}$, $\pi(a) = aH \ \forall a \in G$ (في الزمر)

(في الحلقات)

Def. Let R be a ring and let I an ideal of R define $\mu : R \to R/I$ by $\mu(r) = r + I \ \forall r \in R$

μ is called natural epi.

Remarks:- it is clear

① μ is homo.

② $\ker \mu = I$.

③ μ is ~~[illegible]~~ epi.

Proof ③ Let $h + I \in R/I$ ~~[illegible]~~ To prove μ is epi. We must find $? \in R \Rightarrow \mu(?) = h + I$

$? = h$

Proof ② $\ker \mu = I$ (صفر الحلقة الكسرية مقاسيا.)

$\ker \mu = \{r \in R / \mu(r) = 0\}$ (since $\ker f = \{r \in R / f(r) = 0\}$)

$aH = a$ iff $a \in H$

$= \{r \in R / r + I = I\}$

$r + I = I$ iff $r \in I$

$= \{r \in R / r \in I\}$

$= I$

57

The fundematel Theorm of ring iso.

البرهنات الأساسية في التشاكل الحلقي:-

① First iso. Th.

Let R and R' be Two rings and Let $f: R \to R'$ be an epi. Then:

$$\frac{R}{\ker f} \simeq R'$$

② Second iso. Th.

Let I & J be Two ideals of a ring R Than

$$\frac{I+J}{J} \simeq \frac{I}{I \cap J}$$

③ Third iso. Th.

Let I and J be Two ideal's s.t $I \subseteq J$ Then

$$\frac{R/I}{J/I} \simeq \frac{R}{J}$$

H.W Prove 3rd iso. Th.

(58)

Theorm: Let Z_n & Z_m be Two rings of Z_{nm} If gcd $(m,n)=1$ Then $Z_{nm} \simeq Z_n \oplus Z_m$

Example: Z_6 and Two ideal $Z_2 = \{\bar{0}, \bar{3}\}$ & $Z_3 = \{\bar{0}, \bar{2}, \bar{4}\}$ of Z_6

$\gcd(2,3)=1$

$Z_6 \simeq Z_2 \oplus Z_3$

بالنسبة لهذه البرهنة تطبق Z_n و Z_m على ان $Z_m \nmid Z_n$, $Z_n \nmid Z_m$

Example: $Z_2 = \{\bar{0}, \bar{1}\}$, $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$Z_2 \oplus Z_3 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2})\} \simeq Z_6$

$\because \gcd(2,3)=1 \Rightarrow \underset{6=2(3)}{Z} \simeq Z_2 \oplus Z_3$

لا تطبق هذه البرهنة على مثاليات داخل الحلقة: وانما على حلقات مختلفة Z_n, Z_m ليس بينها علاقة كما ذكر اعلاه.

In genrl for any Two rings Z_n & Z_m iff gcd $(m,n)=1$

$Z_n \oplus Z_m \simeq Z_{nm}$ ان

EX: $Z_2 = \{\bar{0}, \bar{1}\}$, $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$Z_2 \oplus Z_4 \simeq Z_8$ why?

59

Fields :- الحقل

الحقل هو حلقة خاصة تتميز بامتيازات أقوى من التي تتسم بها الساحة.

__Def:-__ A ring R is called field if it is commutative with 1 and every non-zero element of R is invertible (unit)

I.D: Comm. / with 1 / has no zero divisor element.

Fields: comm. / with 1 / Every non zero element of R is unit.

__Examples:-__

1. $\mathbb{R}$ is field.
2. $\mathbb{Q}$ is field.
3. $\mathbb{Z}$ is not field. since:- not every element of $\mathbb{Z}$ is unit. The fact, the only unit element of $\mathbb{Z}$ is 1 & -1
4. $(\mathbb{Z}_p, +_p, \cdot_p)$ is field. $\forall$ prime no. p. such as, $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, ---$ ets.

$(\mathbb{Z}_4, +_4, \cdot_4)$ is not field. , $\mathbb{Z}_4$ not p.no

$(\mathbb{Z}_3, +_3, \cdot_3)$ is field , $\mathbb{Z}_3$ is prim no

Give Prove and Example For The realtion between I.D and Field.

I.D + Every element is unit = Field

So, Field $\longrightarrow$ I.D $\left\{\begin{array}{l}\text{comm.}\\ \text{with 1}\\ \text{has no Zero diver element.}\end{array}\right.$

$\not\Longleftarrow$

Proof. Let R be Field T.P R is I.D

$\Leftarrow$

We have R b Field and T.P R is I.D

By assumption R is comm. and With 1

Let $0 \neq a \in R$ T.P a is non Zero diver element

suppose The Converse $\Rightarrow \exists\, 0 \neq b \in R \Rightarrow ab = 0$ --- ⊛

$\because$ R is Field

$\therefore$ a is unit.

i.e $\exists\, \bar{a}^{1} \in R \Rightarrow a\bar{a}^{1} = \bar{a}^{1} a = 1$

Multiply Two side of ⊛ By $\bar{a}^{1}$.

$\bar{a}^{1}(ab) = 0\,\bar{a}^{1}$

ass. $\Downarrow$

$(\bar{a}^{1}a)b = 0$ $\quad$ // By def of id.

By def. unit $1b = 0 \Rightarrow b = 0$ C!

$\Leftarrow$ Examplie :- not every I.D is Field.

ring $(\mathbb{Z},+,\cdot)$ it is I.D but it is not Field, why:

$2 \in \mathbb{Z}$ s.t $\exists\, \bar{2}^{1} \in \mathbb{Z}$ with $2 \cdot \bar{2}^{1} = 1$

(06b)

Remark:- every Field is integral domain what about The Converse.

كل حقل هو ساحة ماذا عن العكس.
لا يصح العكس ولكن يوجد شرط يصح فيه العكس
يتم طرحه ~~...~~ لاحقاً.

Theorm:- let R be an integral domain whic containg finite Principal ideals Then R is field.

I.D + containg Finite no. of Principal ideals = Field

هذه البرهنة تجعل العكس صحيح I.D → Field عندما تكون R ساحة وتكون
عدد منتهي من المثاليات الرئيسية فهي حقل.
* عند سحب الشرط (Finite) تصبح البرهنة غير صحيحة.

example:- Z is I.D and containg infinit princip ideal but it is not Field.

Example:- Z_5 is field.
I.D has finite Principal ideal
Z_4 is not field.
not I.D and finite Principal ideal.

(69)

Q: under what Condition I.D be field & Prove one of Them.

تذكر البرهنة السابقة مع نتيجة البرهنة التي سوف يتم طرحه الآن وبرهانها.

__Corollary:-__ If R is finit integral domain Then, R is Field.

__Proof:-__

R is called finite ring if it has finite no. of element

$\because R$ is finite

$\therefore$ The number of Principal ideal of R is finite

$\therefore R$ is I.D, So By The ① (Let R be I.D containing Finite Principal ideals Then R is field.)

$\therefore R$ is Field.

نعتبر أيضاً تشخيص آخر للحقل.

Example ① Z_5 is field since it is containing only $\{0\}$ & Z_5.

② Z_8 is not field since is containing Proper ideal $\{0\}$ and $\langle \bar{2} \rangle$ and $\langle \bar{4} \rangle$

③ Z is not Field since it has infinite Proper ideals $nZ = \langle \bar{n} \rangle$

$$\left.\begin{array}{l} Z \supset 2Z \supset 4Z \supset 8Z \cdots \\ Z \supset 3Z \supset 6Z \supset \cdots \end{array}\right\} \text{not Field since } Z \text{ not field.}$$

ومن ايضاً تنتج Z.

(63)

Give anther charcter of field. سنعرض آخر لتعريف الحقل.

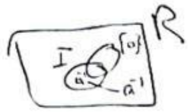
Theorm: Let R be a comm. ring with 1 The R is field if and only if R is contains only Two ideals $\{0\}$ & R.

* R is Field iff cont. Two ideals $\{0\}$ & R itself

" " " " " The Triveal ideal.

The only Proper ideals of R is $\{0\}$.

Proof: $\Rightarrow$ We have R is field T.P R has only trivel ideals $\{0\}$ & R



Let $0 \neq I \overset{ideal}{\leq} R \Rightarrow \exists\, 0 \neq a \in I$

$\because R$ is field $\Rightarrow a$ is unit element.

$\Rightarrow \exists\, a^{-1} \in R \Rightarrow a a^{-1} = a^{-1} a = 1$

$\therefore I$ has a drop property يقال خاصية السحب

$\therefore a a^{-1} \in I$

$1 \in I$ by def of unit.

$I = R$

$\therefore R$ has only Two ideal's $\{0\}$ and R

(68)

⇐ We have R has only $\overline{\text{Two}}$ ideals $\{0\}$ & R T.P R is field.

By assumption, R is comm and with 1 T.P every element of R is unit.

Let $0 \neq a$ T.P a is unit

~~[illegible]~~

Take $\langle a \rangle = \{ra / r \in R\}$

We have $\overline{\text{Two}}$ case!

either! $\langle a \rangle = 0$

$\Rightarrow a \neq 0$ C!

or $\langle a \rangle \neq 0$

By assumption

R with 1 $\langle a \rangle = R$

$\because 1 \in R \Rightarrow 1 \in \langle a \rangle$

$1 = r_0 a$ for some $r_0 \in R$

$\because$ R is comm.

$= a r_0$

So, we have

$1 = r_0 a = a r_0$ تعريف unit

By def of unit element.

$\therefore$ a is unit

$\therefore$ R is Field (By def of Field).